



Department of Homeland Security Daily Open Source Infrastructure Report for 26 October 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The FBI is investigating how classified documents from the Los Alamos Nuclear Laboratory in New Mexico turned up in the home of a subcontractor in Albuquerque. (See item [2](#))
- The Federal Aviation Administration has reprimanded JetBlue Airways Corp. for allowing its pilots to fly more hours than regulations permit in an attempt to study pilot fatigue. (See item [17](#))
- The federal government is investigating a possible major security breach at San Francisco International Airport that may have allowed a knife to be put onboard an American Airlines flight traveling to Miami on Monday, October 23. (See item [18](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *October 25, Arizona Daily Star* — **Truck, tool theft at energy maintenance facility.** Thousands of dollars' worth of vehicles and tools were stolen from a U.S. Department of Energy maintenance facility in Yuma County, AZ. The FBI and the Yuma County Sheriff's Office announced a \$10,000 reward for information that leads to the arrest and conviction of the individual or individuals responsible for the theft. Between 5 p.m. CDT October 20 and 3

p.m. October 21, three specialized vehicles and tools worth more than \$100,000 were taken from the Energy Department Western Power Administration's Gila Substation Maintenance Facility. The tools are used to maintain the high-voltage power grid and its equipment. Special skills and knowledge are required to use the tools and operate the power grid. Two of the vehicles are still missing; one was found abandoned and burned October 21 in Yuma County. All three trucks were modified to carry utility equipment and heavy ladders.

Source: <http://www.azstarnet.com/allheadlines/152608>

2. *October 25, United Press International* — **U.S. nuclear documents seized at New Mexico home.** The FBI is investigating how classified documents from the Los Alamos Nuclear Laboratory in New Mexico turned up in the home of a subcontractor. The find was made last week when the Los Alamos police responded to a domestic violence call, KRQE-TV, Albuquerque, reported Wednesday, October 25. Once in the house, police said they found drug paraphernalia, along with documents that appeared to have been stolen from the nuclear lab, the report said.

Source: <http://www.upi.com/NewsTrack/view.php?StoryID=20061025-064038-7963r>

3. *October 24, Headwaters News (UT)* — **Utah tribe battles to develop own oil.** The Ute Indian reservation is flush with a kind of crude oil called black wax that business leaders can't move to a refinery. The reason: it's of a consistency that makes it economically impossible to ship farther than to refineries along the Wasatch Front. John Jurrius, a Texas oilman who was hired by the tribe to supervise its finances and oil interests is recommending a new refinery. The plan fits well with the nation's push for more energy independence, especially following hurricane Katrina, which shut down several refineries. Jurrius has elicited the help of Utah's state and federal lawmakers, who support the plan for a new refinery that could handle the tribe's increasing inventory of black wax, which produces just as good a final product as other types of crude. The new refinery, they say, could also provide some relief for gas prices in a state that has some of the highest in the nation.

Source: http://www.newwest.net/index.php/topic/article/utah_tribe_battles_the_big_guys_to_develop_own_oil/C35/L35/

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4. *October 25, Fox 41 News (KY)* — **Tanker spill shuts down Shawnee Expressway.** A section of the Shawnee Expressway in Louisville, KY, remains closed after a tanker truck spilled thousands of gallons of gasoline onto the roadway on Tuesday, October 24. All lanes of I-264 and Cane Run Road are shut down at the accident scene. Police say the accident sent nearly 8,000 gallons of gasoline onto the expressway. A hazardous materials crew was dispatched to the scene to mop up and foam the gasoline.

Source: <http://www.fox41.com/article/view/8580/?tf=wdrbarticleview.tpl>

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

5. *October 26, Finextra* — **Customers clean out 'double your money' RBS ATM.** Hundreds of customers waited for up to three hours in Bristol, UK, on Saturday, October 21, to use a faulty cash machine owned by Royal Bank of Scotland (RBS) that started dispensing twice the amount of money requested. According to UK press reports, customers flocked around the ATM as news of the fault spread for a chance to "double their money." Another RBS ATM at the same location, which was operating normally, remained unused. Many customers withdrew cash then waited in line again. The unit eventually ran out of cash Saturday evening. A RBS spokesperson told reporters that due to a "manual error," the machine began dispensing incorrect bills.

Source: <http://finextra.com/fullstory.asp?id=16073>

6. *October 25, Register (UK)* — **ID theft scam hunt goes global.** UK police are working with Interpol in a bid to track down the perpetrators of a malware-powered ID theft scam that has claimed thousands of victims worldwide. As previously reported, a computer seized in the U.S. contained personal data — including names, addresses, credit card information, and transaction records, from at least 2,300 people. Closer examination has revealed the details of at least 8,500 people in 60 countries were obtained through the scam. The data was swiped using key-logging Trojan software, now identified as a variant of Haxdoor, according to the Metropolitan Police's Computer Crime Unit. Login credentials associated with 600 financial companies and banks have been found on the U.S. machine that's at the center of the investigation. The data is contained in 130,000 files, and contains information including login details for ecommerce sites such as eBay, Amazon, and ISPs including BT and Pipex. It's unclear if any money has been stolen from online accounts as a result of the scam. UK police have contacted suspected victims directly by e-mail and alerted banks that particular account numbers have been compromised.

Source: http://www.channelregister.co.uk/2006/10/25/id_theft_scam_hunt/

7. *October 25, Websense Security Labs* — **Multiple phishing alerts: Western Security Bank, Woodforest National Bank, Heritage Bank.** Websense Security Labs has received several reports of a phishing attack that target bank customers. In each incident, an e-mail provides a link to a phishing site that attempts to collect user account information.
- Western Security Bank: Users receive a spoofed e-mail message claiming that new server equipment has been installed at the Bank, and that users must update their records.
- Woodforest National Bank: Users receive a spoofed e-mail message claiming that the bank has implemented a new security system, and that customers must confirm their accounts before the system can be activated.
- Heritage Bank: Users receive a spoofed e-mail message claiming that they must renew their accounts immediately to avoid suspension of online services.

Screenshots:

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=678>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=680>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=681>

Source: <http://www.websense.com/>

8. *October 24, Daytona Beach News-Journal (FL)* — **ATM deposit box stolen; identity theft a concern.** Thieves stole an automatic teller machine deposit box from the drive-through at a SunTrust bank in Daytona Beach, FL, Monday morning, October 23. Police suspect the thieves pried the ATM open sometime after 4:30 a.m. EDT when the bank's cameras turn off, said Deputy Police Chief Ben Walton. Police were concerned that thieves could use information from the stolen deposits for identity theft.

Source: <http://www.news-journalonline.com/NewsJournalOnline/News/EastVolusia/evIEAST05102406.htm>

9. *October 24, Businesswire* — **APWG announces availability of Internet crimeware report.** The Anti-Phishing Working Group (APWG) has issued a joint report with the Department of Homeland Security and SRI International on the role of crimeware in enabling new forms of financial crime on the public Internet. "Crimeware is the latest technological attack on identity and access control on the Internet. Instead of viruses, which were spread largely to gain notoriety for their authors, crimeware is malicious software designed to steal identity information such as passwords and sensitive user information... many organizations are unaware of the scope of this emerging threat," said David Jevans of the APWG. The report details the innovative and penetrating mechanisms that phishers are employing to spread crimeware including: piggybacking schemes in which crimeware is embedded into another piece of software such as an apparent shareware application; Internet worms that exploit vulnerabilities within networks and PCs to propagate themselves and install back doors; and Distribution via Affiliate Marketing in which marketing programs provide incentives to install malware on visitors PCs, some of which can be later exploited to plant crimeware or to directly install crimeware on visitors' PCs.

: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond:

http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf

Source: <http://biz.yahoo.com/bw/061024/20061024005615.html?.v=1>

10. *October 24, ABC News* — **E-mail hoax claims to be from FBI.** The FBI's Internet Crime Complaint Center has warned Internet users and others to be aware of a hoax e-mail that claims to come from FBI Director Robert Mueller and other FBI officials. According to the Internet Crime Complaint Center — or IC3 — notice, the hoax e-mail advises the recipient that he is the beneficiary of a large sum of money. It states further that in order for him to claim the money, the recipient must provide an FBI Identification Record and a Certificate of Ownership. The e-mail contains information lifted from the FBI's Website that describes what an Identification Record is and how to obtain it from the FBI's Criminal Justice Information Services Division. The e-mail concludes with a threatening message that is from FBI Director Robert S. Mueller, III. Later, individuals receive a second, more threatening notice, claiming to come from Donna Uzzell, another senior FBI official, which says, "It has come to the attention of our Money Trafficking investigation department, that you have some funds valued at U.S \$10.5 Million to your name... You are under an observational/Investigation in connection with money laundering."

Source: <http://abcnews.go.com/Technology/print?id=2603777>

11. *October 24, Associated Press* — **Patients told of data mishandling.** The Sisters of St. Francis Health Services, operator of 12 hospitals in Indiana and Illinois, is notifying more than a quarter-million patients that compact discs containing their Social Security numbers and other personal information were lost for three days over the summer. However, officials said they do not believe any of the 260,000 patients' information was improperly accessed. An employee of a medical billing contractor copied the data onto several CDs in July and placed them in a new computer bag to work from home. That employee later decided the bag was too small and exchanged it at a store, accidentally leaving the discs inside. Lisa Decker, a spokesperson for St. Francis subsidiary Greater Lafayette Health Services, said that the person who later bought the bag three days later immediately returned the discs and officials were confident the data was not accessed.

Source: http://news.yahoo.com/s/ap/20061024/ap_on_he_me/hospital_rec_ords_1

[[Return to top](#)]

Transportation and Border Security Sector

12. *October 25, Press-Reporter (AL)* — **Alabama Port Authority approves \$159.2 million budget.** The Alabama State Port Authority approved a \$159.2 million capital budget for 2007 at its regular meeting Tuesday, October 24, including projects that will be partially financed by \$105 million in bond money the authority agreed to borrow earlier this month. The money will be used for infrastructure and equipment that pave the way for anticipated growth, authority officials said. Also during Tuesday's meeting, Hal Hudgins, head of planning and port security, told the board that the docks' closed-circuit security camera system is being tested, and is expected to be fully operational by the end of this calendar year. The security system had been damaged by Katrina before it was fully operational.

Source: <http://www.al.com/business/mobileregister/index.ssf?/base/business/116176843790310.xml&coll=3>

13. *October 25, Associated Press* — **Building fire disrupts Chicago commute.** The Tuesday, October 24, fire that engulfed a vacant building beside a busy Chicago downtown commuter train line — and the danger of collapse — shut down a section of elevated track that serves two Chicago Transit Authority rail lines and disrupted the commute Wednesday morning, October 25, including on the line that connects the Loop to Midway Airport. Officials worried the six-story building might collapse on to the tracks. Kevin Smith, a spokesperson for the city's Office of Emergency Management and Communications, said a "collapse zone" was cordoned off around the brick building, on the south side of Chicago's downtown Loop, for fear it could come crashing down. One firefighter and a civilian were hospitalized in good condition for minor injuries related to the blaze, Fire Department spokesperson Will Knight.

Source: http://hosted.ap.org/dynamic/stories/C/CHICAGO_LOOP_FIRE?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

14. *October 25, USA TODAY* — **Traveler program in demand.** Ten of the U.S.'s busiest airports have asked the federal government if they can start Registered Traveler programs that would give pre-screened passengers a shortcut through security lines. Those programs could begin by the end of the year, launching a much-delayed effort to expedite security for travelers who pass background checks. Atlanta, Chicago O'Hare, and Los Angeles — the nation's three busiest —

have asked the Transportation Security Administration (TSA) to let them run voluntary Registered Traveler programs, along with 19 other airports. The TSA must approve airports and companies that would enroll passengers, provide fingerprint-embedded ID cards and usher registered travelers through security. Carter Morris, a vice president at the American Association of Airport Executives, said programs could start by the end of the year and expand quickly. "It will be a strong start," Morris said. People in Registered Traveler would go through reserved security lanes that may waive procedures such as removing shoes and coats. Airports and travel groups say the program must operate at a significant number of places to attract millions of passengers nationwide.

Source: http://www.usatoday.com/travel/flights/2006-10-24-registered-traveler_x.htm

15. *October 25, Herald Net (WA)* — **Propane truck found in Everett, Washington, after terror alert.** A propane truck stolen from east King County, WA, was found Tuesday morning, October 24, in Everett behind a car rental company. The truck, loaded with 2,500 gallons of propane, was reported stolen about 3 a.m. PDT from Suburban Propane, Everett police Sgt. Boyd Bryant said. A statewide terrorist alert was issued and police around the area were asked to look for the truck. Employees at the rental business recognized the truck from news broadcast and called police. Anyone with information is asked to call the tip line at 425-257-8450.

Source: http://www.heraldnet.com/stories/06/10/25/100loc_b5briefs001.cfm

16. *October 25, USA TODAY* — **Liquids not as risky as first feared.** Passengers will be allowed to carry liquids on airplanes under new security rules prompted by FBI tests that show it's highly unlikely that terrorists could bring down a jet with a bomb made from small amounts of fluids, the nation's airport security chief said Monday, October 23. Travelers may bring liquids and everyday items such as shampoo, toothpaste and makeup through security, provided they're stored in three-ounce containers that fit in a one-quart clear bag, Transportation Security Administration chief Kip Hawley said Monday. Passengers also can carry on liquids and gels in any quantity that they buy in airport shops after passing through security, including at duty-free shops. Testing by the FBI and at government labs showed that small containers of liquids "don't pose a real threat," Hawley said. The TSA banned liquids and gels from carry-on bags August 10 after British authorities reported foiling a plot to destroy U.S.-bound airplanes using liquid explosives. Easing the ban was hailed by the Air Transport Association, an airline trade group, and the National Business Travel Association. Some airlines reported a loss of business since the liquid ban took effect.

For further information on travel items: <http://www.tsa.gov/travelers/index.shtm>

Source: http://www.usatoday.com/travel/flights/2006-09-25-airlines-liquids_x.htm

17. *October 24, Newsday (NY)* — **FAA criticizes JetBlue for pilot-fatigue study.** JetBlue Airways Corp. has been reprimanded by the Federal Aviation Administration (FAA) for allowing pilots to fly more hours than regulations permit in an attempt to study pilot fatigue without permission from high-level FAA officials, the company said Monday, October 23. The airline, one of the nation's leading low-cost carriers, had 29 pilots fly as many as 11 hours a day on more than 50 flights in May 2005 to study alertness, said JetBlue spokesperson Jenny Dervin. FAA regulations allow pilots to fly no more than eight hours a day. Passengers were unaware the pilots had been flying longer than regulations allow. Motion detectors were attached to pilots' wrists. They also used hand-held devices that issued prompts and recorded

response speed. A third pilot was always aboard in case of problems, JetBlue said, adding that none came up. Dervin acknowledged that JetBlue undertook the study without permission from high-level officials at FAA headquarters in Washington, DC. FAA spokesperson Laura Brown said she had not heard of other carriers conducting similar studies.

Source: <http://www.bradenton.com/mld/bradenton/business/15832173.htm>

18. *October 24, CBS News (CA)* — **Knife found on plane from SFO.** The federal government is investigating a possible major security breach at San Francisco International Airport (SFO) that may have allowed a knife to be snuck aboard an American Airlines flight traveling to Miami on Monday, October 23. American Airlines Flight 442 landed at Miami International Airport after a routine five-hour flight from San Francisco around 9 pm EDT Monday. After passengers had already exited the cabin, a member of the airline cleaning crew discovered a blanket left behind. Wrapped inside the blanket was a folding knife with a razor-sharp three-inch blade. The FBI and Transportation Security Administration are investigating the incident and are looking into whether there was a security breach at SFO, including whether screeners examining carry-on items missed the object.

Source: http://cbs5.com/topstories/local_story_298014326.html

19. *October 20, Government Accountability Office* — **GAO-07-16: Commercial Space Launches: FAA Needs Continued Planning and Monitoring to Oversee the Safety of the Emerging Space Tourism Industry (Report).** In 2004, the successful launches of SpaceShipOne raised the possibility of an emerging U.S. commercial space tourism industry that would make human space travel available to the public. The Federal Aviation Administration (FAA), which has responsibility for safety and industry promotion, licenses operations of commercial space launches and launch sites. To allow the industry to grow, Congress prohibited FAA from regulating crew and passenger safety before 2012, except in response to high-risk events. The Government Accountability Office (GAO) evaluated FAA's (1) safety oversight of commercial space launches, (2) response to emerging issues, and (3) challenges in regulating and promoting space tourism and responding to competitive issues affecting the industry. GAO reviewed FAA's applicable safety oversight processes and interviewed federal and industry officials. If the Department of Transportation (DOT)'s commissioned report on dual safety and promotion roles does not fully address the potential for a conflict of interest, GAO suggests that Congress revisit FAA's promotional role and decide whether it should be eliminated. GAO recommends that FAA assess its future safety oversight resource needs and identify the circumstances that would trigger passenger safety regulation before 2012. Relevant federal agencies reviewed the draft and DOT agreed with the recommendations.

Highlights: <http://www.gao.gov/highlights/d0716high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-16>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

20. *October 25, Daily Beacon (University of Tennessee)* — **Vet school gets security grant.** The University of Tennessee's College of Veterinary Medicine (UTCVM) has stepped onto the national platform for terror defense. On October 16, U.S. Representative Zach Wamp (R-TN) announced the creation of the Center for Agriculture and Food Security and Preparedness (CAFSP) to combat agroterrorism and bioterrorism. The Department of Homeland Security awarded the UTCVM a grant of \$2 million in order to establish within the center an extensive, Web-accessible training program for national and industrial use. The goal of the new center will be to serve as a headquarters for information that will assist the nation in protecting its agriculture and food supply. The government has recognized agriculture and the nation's food supply as potential targets of terrorism, both on a pragmatic level that the consumption or use of targeted livestock and crops could be directly harmful to individuals, as well as on an economic level. In the future, the CAFSP will be the organization in charge of evaluating possible targets and making them less penetrable and more defendable. It will also be an authority on agroterrorism awareness and training.
Source: <http://dailybeacon.utk.edu/showarticle.php?articleid=50697>
21. *October 24, Agriculture Online* — **APHIS approves new Boehringer Ingelheim circovirus vaccine.** Boehringer Ingelheim Vetmedica, Inc., (BIVI) announced this week that it has received approval from the U.S. Animal and Plant Health Inspection Service for a new vaccine called Ingelvac CircoFLEX to protect swine against diseases caused by porcine circovirus type-2 (PCV2). According to Klaas Okkinga, BIVI marketing manager, Ingelvac CircoFLEX is a single-dose vaccine that provides efficacy and safety to pigs. "It's effective in immunizing pigs as young as three weeks of age prior to exposure to PCV2, and provides protection without the systemic irritation and tissue reactions some vaccines can cause," Okkinga says.
Source: <http://www.agriculture.com/ag/story.jhtml?storyid=/templatedata/ag/story/data/1161701822181.xml&catref=ag1001>
22. *October 24, Animal and Plant Health Inspection Service* — **USDA prohibits imports from Canada and interstate movements of fish susceptible to viral hemorrhagic septicemia.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service issued an emergency order Tuesday, October 24, prohibiting the importation of certain species of live fish from Ontario and Quebec, Canada, into the U.S. and the interstate movement of the same species from the eight states bordering the Great Lakes due to outbreaks of viral hemorrhagic septicemia (VHS). This action is in response to the rapid spread of VHS in the Great Lakes region and the potential impact on a growing number of fish species. VHS is a destructive pathogen that produces clinical signs in fish including internal hemorrhaging and death. The disease does not pose a risk to people, but it has been found to affect a number of fish species previously not known to be susceptible including baitfish species, Coho salmon and channel catfish.
Emergency order: http://www.aphis.usda.gov/vs/aqua/pdf/vhs-fed-order_ogc-changes.pdf
Source: <http://www.aphis.usda.gov/newsroom/content/2006/10/vhsfish.shtml>
23. *October 24, Stop Soybean Rust News* — **Twenty-six new soybean rust counties in last 30 hours.** Between 6:00 a.m. EDT Monday, October 23, and 12:00 p.m. EDT Tuesday, October 24, 26 new counties in six states joined the list of those positive for soybean rust in the U.S.,

taking the national total to 205 positive counties and parishes in 15 states. The states with the biggest increases since Monday morning are Tennessee, with nine new counties; Virginia with seven and Arkansas with five. North Carolina reported three more, while Illinois and Mississippi added one each.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=995>

[\[Return to top\]](#)

Food Sector

24. *October 25, USAgNet* — **Japan may accept stored U.S. beef.** The Japanese government indicated over the weekend it may give customs clearance to a shipment of U.S. beef that has been in storage since January. The shipment of about 900 tons of U.S. beef arrived in Japan in January, right before Tokyo implemented a second ban on U.S. beef because of banned parts found in a veal shipment from the U.S., reports MeatNews.

Source: <http://www.usagnet.com/story-national.php?Id=2218&yr=2006>

[\[Return to top\]](#)

Water Sector

25. *October 25, Reuters* — **Australian drought sparks new crime of water theft.**

Drought-ravaged Australian farmers heading into summer are facing a new and previously unknown threat: water bandits. Police at tiny Gundaroo village near the Australian capital Canberra on Wednesday, October 25, said they were hunting thieves who used crowbars to crack open water tanks and steal the precious contents. In nearby Bungendore, water has been stolen from village dams and tanks, while 35 miles away in Yass police have reports of theft from the city's near-dry river. More than 90 percent of the most populous state of New South Wales is in drought, with many farmers enduring five continuous years of below average rainfall. The area around Gundaroo and the nearby town of Goulburn have been particularly hard-hit, with Goulburn's main dam having run dry. Police in the regional Goulburn headquarters said they were investigating several incidents of water theft and advised people to lock their water stores as summer draws closer.

Source: <http://today.reuters.com/News/CrisesArticle.aspx?storyId=SYD 206550>

26. *October 23, KSBY (CA)* — **California well was poisoned.** A San Luis Obispo, CA, jury found Ralph Yates guilty of one count of poisoning his neighbors' well. James Cross, called the Sheriff's Department after he says he saw Yates on a ladder, standing over his well in May 2005. Investigators discovered a soiled, white plastic bag, newspaper and toilet paper inside the well. Tests confirmed it was human waste. The well became contaminated with E. coli. The Cross family made more than \$20,000 worth of changes. They installed video equipment, put in a new water tank closer to their home and bought guard dogs. They also started to only drink bottled water. Meantime, their case slowly made its way through the legal system.

Source: <http://www.ksby.com/home/headlines/4462472.html>

27.

October 23, LiveScience — **DNA found in drinking water could aid germs.** DNA that helps make germs resistant to medicines may increasingly be appearing as a pollutant in the water. This DNA was found "even in treated drinking water," researcher Amy Pruden, an environmental engineer at Colorado State University, told LiveScience. Experts note that up to 95 percent of antibiotics are excreted by humans and animals unaltered, seeping into the environment and encouraging antibiotic resistance there. Pruden's new research did not focus on the presence of antibiotics in the environment. Instead, she looked for the presence of genes that help confer drug resistance to the germs in the first place. Bacterial genes are encoded as DNA, and microbes often swap genes with each other. In principle, antibiotic-resistance genes could persist and spread long after the drugs they target have dissipated. Pruden and her colleagues investigated a range of northern Colorado waters, from pristine river sediments to water from dairy lagoons to irrigation ditches. They also looked at water from drinking-water treatment plants and effluents from a wastewater recycling plant. Researchers discovered the presence of antibiotic-resistance genes in all the waters they investigated.

Source: <http://msnbc.msn.com/id/15392046/>

[[Return to top](#)]

Public Health Sector

28. *October 25, Agence France-Presse* — **Malaria vaccine may be ready by 2010.** The first vaccine against malaria could be on the market by 2010 following trials in Mozambique, the southern African country's deputy health minister told an international conference on Tuesday, October 24. Mozambican officials announced in July 2002 that they had begun testing a drug that could be developed into a malaria vaccine on several people.

Source: http://www.iol.co.za/index.php?set_id=14&click_id=117&art_id=qw1161723429736B252

29. *October 25, Agence France-Presse* — **Wasteful diagnoses fail to trace tuberculosis in worst affected areas.** Large amounts of money are being wasted on ill-conceived diagnostic tools for tuberculosis (TB) that are failing to trace the disease in poor areas where they are most needed, the World Health Organization (WHO) has said in a report. Most of the estimated nine million people who develop active TB every year do not receive a laboratory-confirmed diagnosis even though about one billion dollars is spent annually on TB tests and evaluations, the report found. By comparison, 300 million dollars is spent on drugs to treat TB worldwide. About 1.7 million people succumb to the disease every year, many of them because the infection is not diagnosed or is discovered too late, the WHO said. The report said improved tests could bolster international control of the disease, which is expanding, and help tackle the growing threat of multi-drug resistance.

Diagnostics for Tuberculosis: http://www.who.int/tdr/TBDI_full.pdf

Source: http://news.yahoo.com/s/afp/20061025/hl_afp/healthtuberculosiswho_061025115933

[[Return to top](#)]

Government Sector

30. *October 25, NBC News (CA)* — Threat continues; Diablo Valley College to stay closed.

Diablo Valley College spokesperson Chrisanne Knox said the school would remain closed Wednesday, October 25, after a weekend bomb threat caused extra security Monday and a complete shutdown Tuesday. Dogs identified two suspicious locations, which were searched and determined safe Tuesday afternoon, according to Knox. "The bomb dogs found something for us today to look at so that's why it was more specific and it's better to err on the side of caution," said one police officer. Knox said that the bomb squad conducted a controlled explosion in an attempt to open a locker outdoors near the Diablo Valley College quad in Pleasant Hill, CA. Although the suspected areas were deemed safe, the threat isn't completely resolved, Knox said. Police will guard the campus through Tuesday night and all of Wednesday. Police said the caller mentioned a three-day period, so they're being extra cautious. Knox said a full investigation will be done and if the caller is caught, he or she will face stiff penalties. Federal officials assisted local authorities in the investigation. Diablo Valley College is the No. 1 transfer community college to University of California– Berkeley.

Source: <http://www.nbc11.com/news/10145686/detail.html>

[\[Return to top\]](#)

Emergency Services Sector

31. *October 25, Federal Emergency Management Agency* — Federal Emergency Management Agency National Situation Update.

Tropical Weather Outlook: Central and Eastern Pacific: Outer squalls associated with Tropical Storm Paul are affecting southern Baja, CA, and a Tropical Storm warning remains in effect for the area. At 5:00 a.m. EDT the center of Paul was located about 75 miles south of Cabo San Lucas, Mexico. Earthquake Activity: At 5:26 p.m. EDT Tuesday, October 24, there was a light (4.4) magnitude earthquake centered 42 miles west of Petrolia, CA, and was 3.9 miles deep in the crust. No reports of injuries or damage have been received. At 1:58 a.m. EDT Tuesday, there was a light (3.5) magnitude earthquake centered 41 miles west-southwest of Rincon, Puerto Rico. No reports of injuries or damage have been received. Swarm of Earthquakes Reported Near Old Faithful: A swarm of more than 70 small earthquakes shook the ground near Old Faithful geyser earlier this month. The largest was a magnitude 2.4, barely enough to be felt. The swarm of 74 quakes lasted several hours on Saturday, October 14, according to information recently released from the Yellowstone Volcano Observatory.

To view other Situation Updates: <http://www.fema.gov/emergency/reports/index.shtm>

Source: <http://www.fema.gov/emergency/reports/2006/nat102506.shtm>

32. *October 24, Federal Emergency Management Agency* — President declares major disaster for New York.

The head of the Department of Homeland Security's Federal Emergency Management Agency announced Tuesday, October 24, that federal disaster aid has been made available for the state of New York to supplement state and local recovery efforts in the area struck by severe storms and flooding during the period of October 12–13, and continuing.

For more information: <http://www.fema.gov/news/event.fema?id=7225>

Source: <http://www.fema.gov/news/newsrelease.fema?id=31021>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

33. *October 24, Security Focus* — MySQL MERGE privilege revoke bypass vulnerability.

MySQL is prone to a vulnerability that allows users with revoked privileges to a particular table to access these tables without permission. This issue allows attackers to gain access to data when access privileges have been revoked. The specific impact of this issue depends on the data that the attacker may retrieve.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/19279/info>

Solution: The vendor released versions 4.1.21 and 5.0.24 (to be released) to address this issue.

For more information: <http://www.securityfocus.com/bid/19279/references>

Source: <http://www.securityfocus.com/bid/19279/discuss>

34. *October 24, CNET News* — Florida man charged in botnet attack on Akamai. A Florida man has been charged with launching a distributed denial-of-service attack against servers run by Akamai Technologies. A federal court in Boston on Tuesday, October 24, heard charges that 32-year-old John Bombard of Seminole used a variant of the Gaobot e-mail worm to turn computers — including systems at two universities whose names have not been disclosed — into an arsenal of "zombies" or "bots" that he could control remotely. He then used this network of hijacked computers, known as a "botnet," to send a massive amount of traffic to the domain name system servers of the Global Traffic Management division of Akamai, prosecutors alleged. This distributed denial-of-service attack, launched June 15, 2004, rendered many of Akamai's clients' Websites temporarily inaccessible, according to the charges.

Source: http://news.com.com/Florida+man+charged+in+botnet+attack+on+Akamai/2100-7350_3-6129226.html?tag=nefd.top

35. *October 24, eWeek* — FBI: Companies need to report cyber attacks. Companies should do more to report cyber-crimes such as hacking and phishing to help federal authorities investigate and ensure that additional data isn't compromised beyond initial attacks, a high-ranking FBI official said. "A huge issue for us is the underreporting of successful or almost successful hacking," Special Agent Mark Merishin, the assistant director-in-charge of the FBI's New York City Office, told a crowd gathered at the Infosecurity Conference and Exhibition on Tuesday, October 24. The agency is troubled by a pattern of behavior among corporations and businesses who are not consistently reporting when their infrastructure has been hacked, or even when their companies have become the unsuccessful target of hackers and other cyber-crooks. Most companies, Merishin said, worry about the bottom line and feel any publicity or investigation into a cyber-crime will hurt profits.

Source: <http://www.eweek.com/article2/0,1895,2036619,00.asp>

36. *October 24, New York Times* — At U.S. borders, laptops have no right to privacy. Many business travelers are walking around with laptops that contain private corporate information that their employers really do not want outsiders to see. Until recently, their biggest concern was that someone might steal the laptop. But now there's a new worry — that the laptop will be seized or its contents scrutinized at United States customs and immigration checkpoints upon entering the United States from abroad. Although much of the evidence for the confiscations remains anecdotal, it's a hot topic this week among more than 1,000 corporate travel managers and travel industry officials meeting in Barcelona at a conference of the Association of Corporate Travel Executives. Last week, an informal survey by the association, which has

about 2,500 members worldwide, indicated that almost 90 percent of its members were not aware that customs officials have the authority to scrutinize the contents of travelers' laptops and even confiscate laptops for a period of time, without giving a reason. Laptops may be scrutinized and subject to a "forensic analysis" under the so-called border search exemption, which allows searches of people entering the United States and their possessions "without probable cause, reasonable suspicion or a warrant," a federal court ruled in July.

Source: http://www.nytimes.com/2006/10/24/business/24road.html?_r=1&oref=slogin

- 37. *October 24, IDG News Service* — Mozilla releases Firefox 2.0.** Just two weeks after Microsoft delivered its highly anticipated Internet Explorer 7, Mozilla has shipped a major update to its Firefox browser. Firefox 2.0 was officially released just after 2 p.m. PDT on Tuesday, October 24, a day after an early version of the software was leaked onto Mozilla's File Transfer Protocol site.

Firefox 2.0 can be downloaded at: <http://www.mozilla.com/en-US/firefox/>

Source: http://www.infoworld.com/article/06/10/24/HNfirefox2.0_1.htm

- 38. *October 24, CNET News* — Microsoft's free anti-spyware hits the market.** Microsoft announced on Tuesday, October 24, the general release of its free anti-spyware program, a move that significantly steps up the software maker's competitive challenge in the security industry. Windows Defender anti-spyware is now available in English to Windows XP users, with other languages set for delivery in coming weeks. Windows Defender will also be bundled with Windows Vista, Microsoft's next-generation operating system, when it is released in January.

Windows Defender anti-spyware:

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

Source: http://news.com.com/Microsofts+free+anti-spyware+hits+market/2100-1029_3-6128978.html

- 39. *October 24, Computer World* — Exploit in Asterisk PBX software patched.** A vulnerability in the Asterisk PBX server that enables an attacker to gain complete control of a PBX system has been discovered by the Australian and New Zealand security outfit, Security-Assessment.com. The exploit allows an attacker to spoof caller IDs, sniff voice calls on the network and take complete control of the system. No public exploits of the vulnerability have been released. Asterisk was notified of the discovery on Tuesday, October 17. A patch for the vulnerability was released by Asterisk on Wednesday, October 18.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004381&source=rss_topic85

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	6346 (gnutella-svc), 1026 (win-rpc), 4662 (eDonkey2000), 44913 (---), 6881 (bittorrent), 37130 (---), 65530 (WindowsMite), 25 (smtp), 1027 (icq), 139 (netbios-ssn)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

40. *October 25, Siskiyou Daily News (CA)* — **Bomb scare investigation continues in Yreka, California.** On Wednesday, October 25, three law enforcement agencies were searching the evacuated Timber Products complex for a bomb after an anonymous 911 caller alerted them. According to Yreka Police Chief Brian Bowles, when the dispatch got the call, they notified Timber Products and the Siskiyou County Sheriff's Office and the California Highway Patrol, Yreka division. Timber Products was evacuated, and a search by officers in all three agencies commenced. Bowles said that a mutual aid request for canine units had gone out throughout the north state area.

Source: <http://www.siskiyoudaily.com/articles/2006/10/24/news/doc453e9498b95c1021190119.txt>

41. *October 23, USA TODAY* — **Crooked builders hit storm victims.** Unlicensed contractors are preying on Gulf Coast residents whose homes were ravaged by Hurricane Katrina and are in dire need of repair, state and FBI officials say. "There's not enough skilled labor out there, and it's causing chaos," says Charles Marceaux, executive director of the Louisiana State Licensing Board for Contractors. Phony contractors are collecting down payments for work and then disappearing, Marceaux says. One scam involves workmen who take down payments and even drop materials off at work sites, only to return in the night to retrieve the materials and sneak away. Marceaux said there are an estimated 20,000 licensed contractors in New Orleans alone. Getting an exact tally of how many unlicensed repairmen are operating is impossible, but he estimates that their number exceeds that of legitimate contractors. James Bernazzani, the FBI's special agent in charge in New Orleans, says the federal government will have jurisdiction in many cases because the money the contractors took often comes from federal rebuilding grants. "Before the storm, the threshold for the FBI to take a fraud case was \$1 million," he says. "But we're assuming non-traditional roles down here, and we're trying to be a deterrent."

Source: http://www.usatoday.com/news/nation/2006-10-23-gulf-coast-contractors_x.htm

42. *October 23, Dallas Morning News* — **Suspicious containers close downtown Dallas streets.** Several streets were closed in downtown Dallas for more than three hours Monday afternoon, October 23, after police and fire officials found two suspicious containers outside the A. Maceo Smith Federal Building near the Dallas Convention Center. Dallas Fire-Rescue Lt. Joel Lavender said an anonymous individual called Dallas Fire-Rescue around 8 a.m. CDT and directed them to check on suspicious objects in the vicinity of the building. Dallas police bomb squad officers, a Dallas Fire-Rescue hazardous materials unit, Federal Protective Service and FBI personnel were called to the scene. After the police examined one container with a robot and firefighters sampled the fluid from both jugs, Lt. Lavender said the liquid was determined to be mostly water with a small amount of alcohol and another inert substance.

Source: <http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/st>

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:
<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.